CLAIMS:

1. A method of preserving privacy for a user while enabling the user controlled access to data,

the user being represented by a user device (110,721) and identified by a user identity,

the method using at least one certificate that associates data access rights with the user identity,

wherein the certificate conceals the user identity,

the certificate comprises publicly available solution information P, and

a concealed secret S' is publicly available,

the method further comprises at least one of

- a certificate verification process (120,420) between the user device and a verifier device (111,701),
- a certificate issuing process (220,520,620) between the user device and an issuing device (211,711), and
- a certificate re-issuing process (320) between the user device and the issuing device,

wherein the certificate verification process comprises the steps of

- the user device obtaining the concealed secret S' corresponding to the certificate,
- the user device retrieving the secret *S* from the concealed secret *S'*,
- the verifier device obtaining the solution information P from the certificate,
- the user device proving to the verifier device that it knows the secret S without the verifier device learning the secret S or the user identity,

wherein the certificate issuing process comprises the steps of:

- generating a secret *S* and a solution information *P*,
- concealing the secret *S* into a concealed secret *S'*,
- the issuing device issuing a certificate comprising at least the solution information *P*,

wherein the certificate re-issuing process comprises the steps of

- the user device obtaining the concealed secret S' corresponding to the certificate,
- the user device retrieving the secret *S* from the concealed secret *S'*,
- the issuing device obtaining the solution information P from the certificate,
- the user device proving to the issuing device that it knows the secret S without the issuing verifier device learning the secret S or the user identity,
- generating a new secret S2 and new solution information P2,
- concealing the secret *S2* into a concealed secret *S2'*,
- the issuing device issuing a new certificate comprising at least the new solution information *P2*.

2. The method according to claim 1, wherein the certificate comprises publicly available concealed secret *S'*.

3. The method according to claim 2, wherein the secret *S* is encrypted with the user's public key to generate the concealed secret *S'*.

4. The method according to claim 1, wherein the solution information P and the secret S are members of Zn*, and the solution information P is the square of S.

5. The method according to claim 1, wherein the concealed secret S' comprises random information RAN.

6. The method according to claim 1, wherein the verifier device verifies that the user device has knowledge of the secret *S* using a zero-knowledge protocol.

7. The method according to claim 1, wherein the communication during the issuing process is protected using symmetric key encryption.

8. The method according to claim 1, wherein in the issuing process the secret S and the solution information P is generated by the user device.

9. The method of claim 1, wherein the certificate is an authorization certificate.

10. The method of claim 1, wherein the certificate is a domain certificate.

11. The method according to claim 10, wherein the concealed secret S' in the domain certificate comprises the secret S, encrypted with the secret domain key.

12. The method according to claim 9, wherein the concealed secret S' comprises the secret S, multiplied with cr_id.

13. The method according to claim 1, wherein the certificate comprises two secrets, of which the knowledge prove by a user device gives different access levels.

14. User device (110,721) being arranged for issuing a certificate according to claim 1, comprising:
- receiving means (727) for receiving process information,
- computing means (722), comprising processing (723), encryption/decryption (725) and storing means (724), for engaging in at least one of the certificate verification process, the certificate issuing process, and certificate re-issuing process, and
- transmitting means (726) for transmitting process information.

15. Verifier device (111,701) being arranged for verifying a certificate according to claim 1, comprising:
- receiving means (707) for receiving process information,
- computing means (702), comprising processing (703), encryption/decryption (705) and storing means (704), for engaging in the certificate verification process, and
- transmitting means (706) for transmitting process information.

16. Issuing device (211,711) being arranged for issuing a certificate according to claim 1, comprising:
- receiving means (717) for receiving process information,
- computing means (712), comprising processing (713), encryption/decryption (715) and storing means (714), for engaging in at least one of the certificate issuing process and certificate re-issuing process, and
- transmitting means (716) for transmitting process information.

17. Signal carrying at least part of a certificate as used in the method according to claim 1.

18. A computer program product (732) carrying computer executable instructions comprising a computer readable medium, having thereon computer program code means, to make a computer execute, when said computer program code means is loaded in the computer, implementing at least one protocol side of at least one of:

- the certificate issuing protocol,
- the certificate re-issuing protocol, and
- the certificate verification protocol.